Home > News > Security > LiteBit Bitcoin Exchange Hacked Twice in Two Months

35

LiteBit Bitcoin Exchange Hacked Twice in Two Months

By **Catalin Cimpanu** September 18, 2017 02:55 AM **0**

LiteBit.eu — a multi-currency exchange based in the Netherlands — has suffered data breaches two months in a row.

According to emails sent to affected customers after each event, no Bitcoin or altcoin funds were stolen in any of these two incidents.

XM
WWW.XM.COM
Get your
$30
Trading Bonus*
Read More
*T&Cs apply. Forex and CFD trading is high risk and can result in the loss of all your invested capital.
USAIN BOLT
OFFICIAL SPONSOR

The company says the attacker only pilfered user personal information, such as emails, hashed passwords, bank account numbers (IBANs), telephone numbers, and home addresses.

While LiteBit was lucky that no currency was stolen, it shows a continued lack of security precautions being taken by exchanges who keep reporting breaches. Furthermore, the information being stolen is obviously of concern to the victims as it could lead to identity theft or to other accounts being hacked by the attackers

August 2017 breach

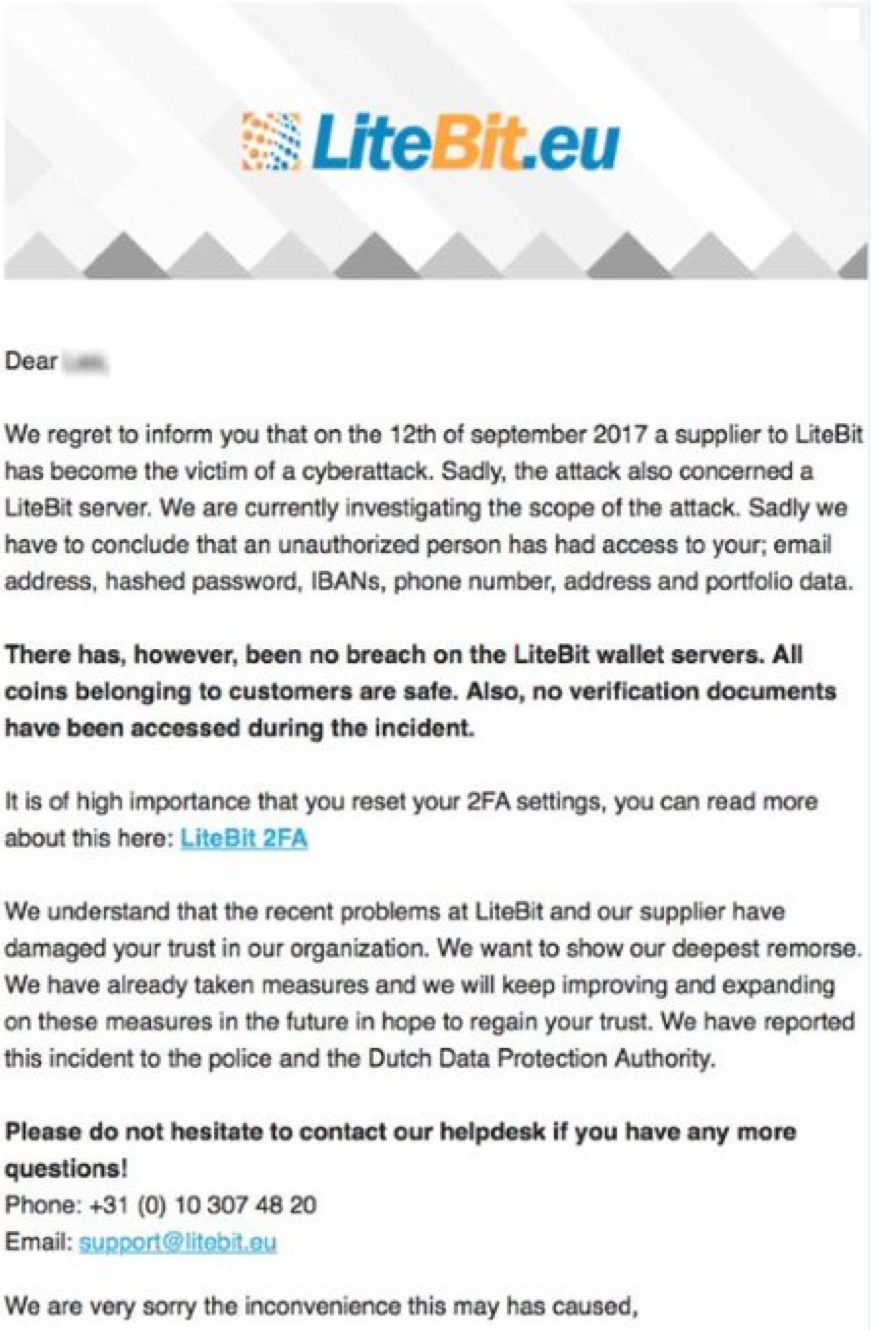
The first incident took place on August 5, and the company sent out the following email to affected customers after it detected suspicious activity on one of its servers and fixed the security hole.

> On August 5, 2017 we observed unusual activities on LiteBit's servers. Unfortunately, we have concluded that there has been unlawful access to LiteBit data. No LiteBit wallet servers have been broken, all coins of customers are safe. Also, there are no verification documents (ID or passport) involved in this incident.
>
> The cause of the leak is known, and the problems have now been solved. It is not clear whether data has actually been stolen. In the worst case, an unauthorized person has gained access to yours; Email address, encrypted password, IBAN, phone number, address and your portfolio data.
>
> What does this mean to you? For users who have 2-step authentication, it's very important that they reset it. We also recommend that you enable this additional security measure, for customers who have not already done so.
>
> In addition, it is important to change your password regularly.

September 2017 breach

The second breach took place last week, on September 12, six weeks after the first incident. This time around, the source of the breach was with one of LiteBit's "suppliers."

Again, the exchange said the hacker made off only with PII and user funds remained secure. Authorities have been informed. The content of the second email is below.



Dear [redacted]

We regret to inform you that on the 12th of september 2017 a supplier to LiteBit has become the victim of a cyberattack. Sadly, the attack also concerned a LiteBit server. We are currently investigating the scope of the attack. Sadly we have to conclude that an unauthorized person has had access to your; email address, hashed password, IBANs, phone number, address and portfolio data.

There has, however, been no breach on the LiteBit wallet servers. All coins belonging to customers are safe. Also, no verification documents have been accessed during the incident.

It is of high importance that you reset your 2FA settings, you can read more about this here: LiteBit 2FA

We understand that the recent problems at LiteBit and our supplier have damaged your trust in our organization. We want to show our deepest remorse. We have already taken measures and we will keep improving and expanding on these measures in the future in hope to regain your trust. We have reported this incident to the police and the Dutch Data Protection Authority.

Please do not hesitate to contact our helpdesk if you have any more questions!
Phone: +31 (0) 10 307 48 20
Email: support@litebit.eu

We are very sorry the inconvenience this may has caused,

Catalin Cimpanu
@campuscodi

LiteBit email announcing September 2017 data breach (h/t anonymous tipster)

2:41 PM - Sep 18, 2017

3 See Catalin Cimpanu's other Tweets

> We regret to inform you that on the 12th of september 2017 a supplier to LiteBit has become the victim of a cyberattack. Sadly, the attack also concerned a LiteBit server. We are currently investigating the scope of the attack. Sadly we have to conclude that an unauthorized person has had access to your; email address, hashed password, IBANs, phone number, address and portfolio data.
>
> There has, however, been no breach of the LiteBit wallet servers. All coins belonging to customers are safe. Also, no verification documents have been accessed during the incident.
>
> It is of high importance that you reset your 2FA settings, you can read more about this here: LiteBit 2FA.
>
> We understand that the recent problems at LiteBit and our supplier have damaged your trust in oour organization. We want to show our deepest remorse. We have already taken measures and we will keep improving and expanding on these measures in the future in home to regain trust your trust. We have reported this incident to the police and the Dutch Data Protection Authority.

BITCOIN CRYPTOCURRENCY DATA BREACH SECURITY BREACH

CATALIN CIMPANU

Catalin Cimpanu is the Security News Editor for Bleeping Computer, where he covers topics such as malware, breaches, vulnerabilities, exploits, hacking news, the Dark Web, and a few more. Catalin previously covered Web & Security news for Softpedia between May 2015 and October 2016. The easiest way to reach Catalin is via his XMPP/Jabber address at campuscodi@xmpp.is. For other contact methods, please visit Catalin's author page.

PREVIOUS ARTICLE NEXT ARTICLE

Post a Comment

Community Rules

You need to login in order to post a comment

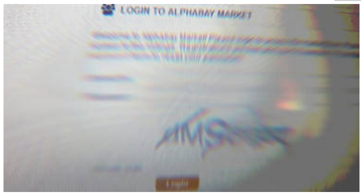
Login

Not a member yet? Register Now

You may also like:

Polish Authorities Confirm Hack of Bitcurex Bitcoin...

bleepingcomputer.com



Man Pleads Guilty to Stealing Bitcoin From Other Dark Web...

bleepingcomputer.com

Hacker Steals $7 Million Worth of Ethereum From...

bleepingcomputer.com

Bitcoin Exchange Shuts Down After Getting Hacked a...

bleepingcomputer.com

BTC-e Owner Arrested for Laundering Stolen Bitcoin, Ransomware...

bleepingcomputer.com

RECOMMENDED VIDEOS

macOS Bug Demo of No

Let's Take a Look at the

macOS High Sierra Bug

Anti-Israel IsraBye Data

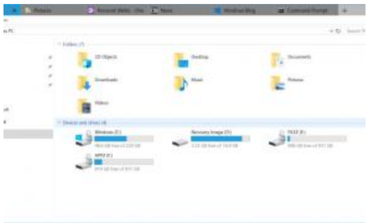
Unwanted Chrome

Add Extension to Leave

VIEW MORE

POPULAR STORIES

Hardcoded Password Found in Cisco Software



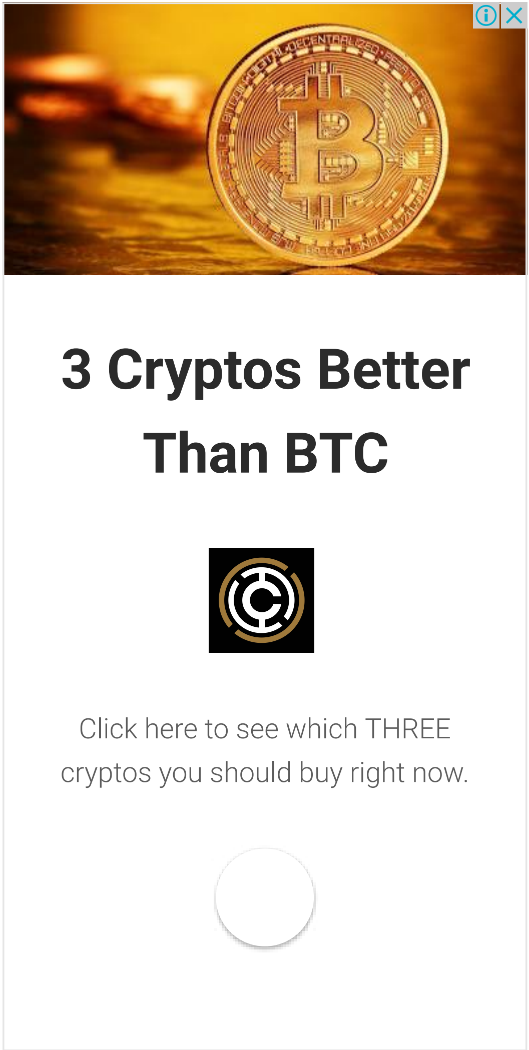
Windows 10 Finally Adding Tabs to File Explorer!

NEWSLETTER SIGN UP

To receive periodic updates and news from BleepingComputer, please use the form below.

Email Address...

Submit



NEWSLETTER SIGN UP

MAIN SECTIONS

News

Downloads

Virus Removal Guides

Tutorials

Startup Database

Uninstall Database

File Database

Glossary

COMMUNITY

Forums

Forum Rules

Chat

USEFUL RESOURCES

Welcome Guide

Sitemap

COMPANY

About BleepingComputer

Contact Us

Advertising

Write for BleepingComputer

Social & Feeds

Changelog

User Agreement - Privacy Policy